Note: Before doing this lab, please create an Instance and storage bucket.

There is a document to create an instance and storage bucket.

Account and Scopes

**Introduction:**

Access scopes are the technique of identifying permissions for your instance. They describe the default OAuth scopes used in requests from the gcloud tool.

You should set up access scopes when you form an instance to run as a service account.

**Problem:**

*You will be working with GCP service accounts and scopes in this lab. You will first work with the bucket ID, and with the help of the bucket ID, you will create storage scopes. First, you will create only a* ***read storage scope.***

**Solution:**

You will first log in to the GCP console using your credentials, and then you will learn how to create instances and link bucket ID with it.

**Step1:** You need to verify that the ***Compute Engine default service account*** member has the ***Editor*** Role.

1. Once you first log in, your screen should look similar to this.



1. Click on the project selector drop-down menu at the top of the screen.



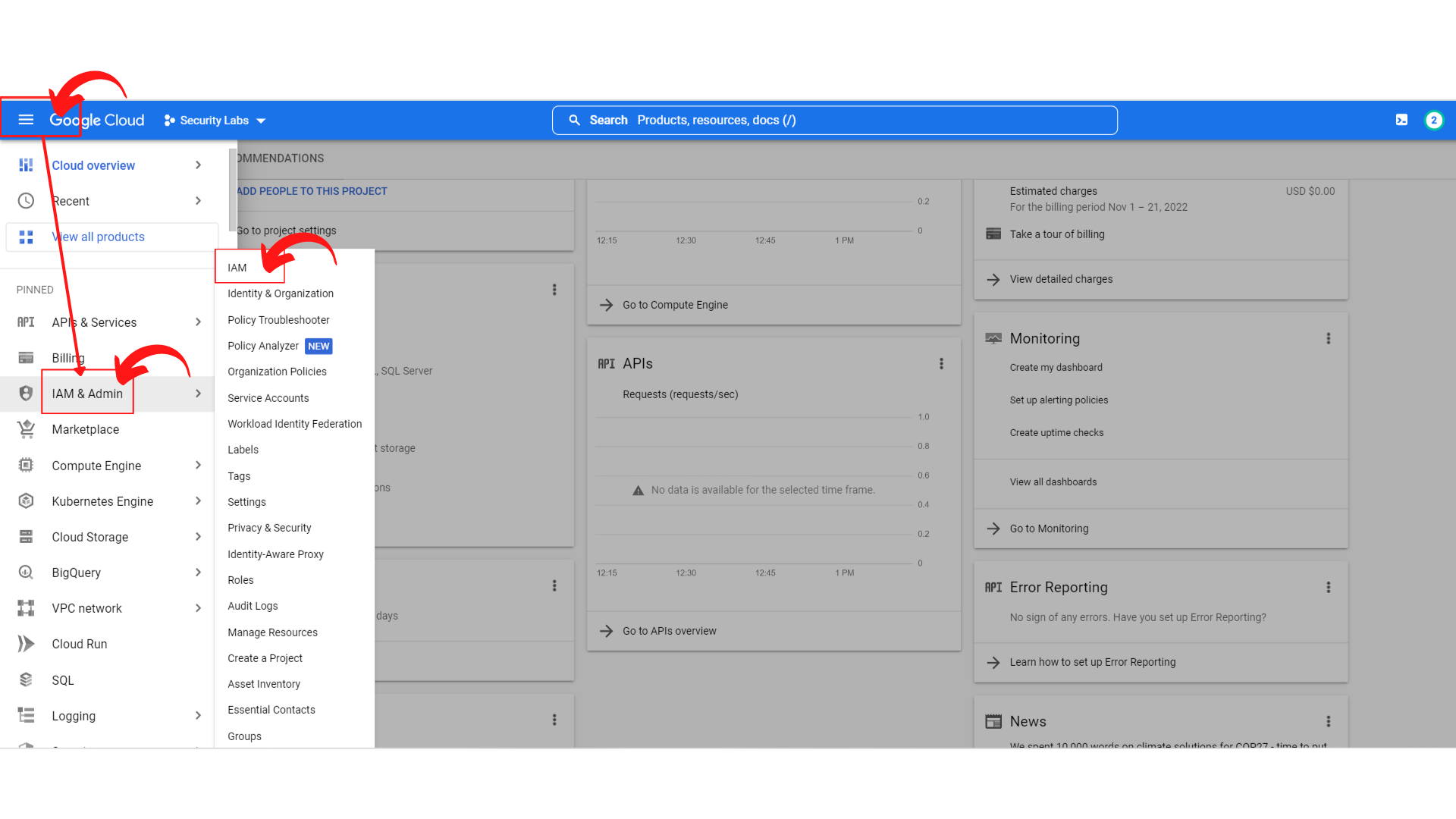
1. Since, we are doing labs on a Security Labs project, Click on *“Security Labs”*.



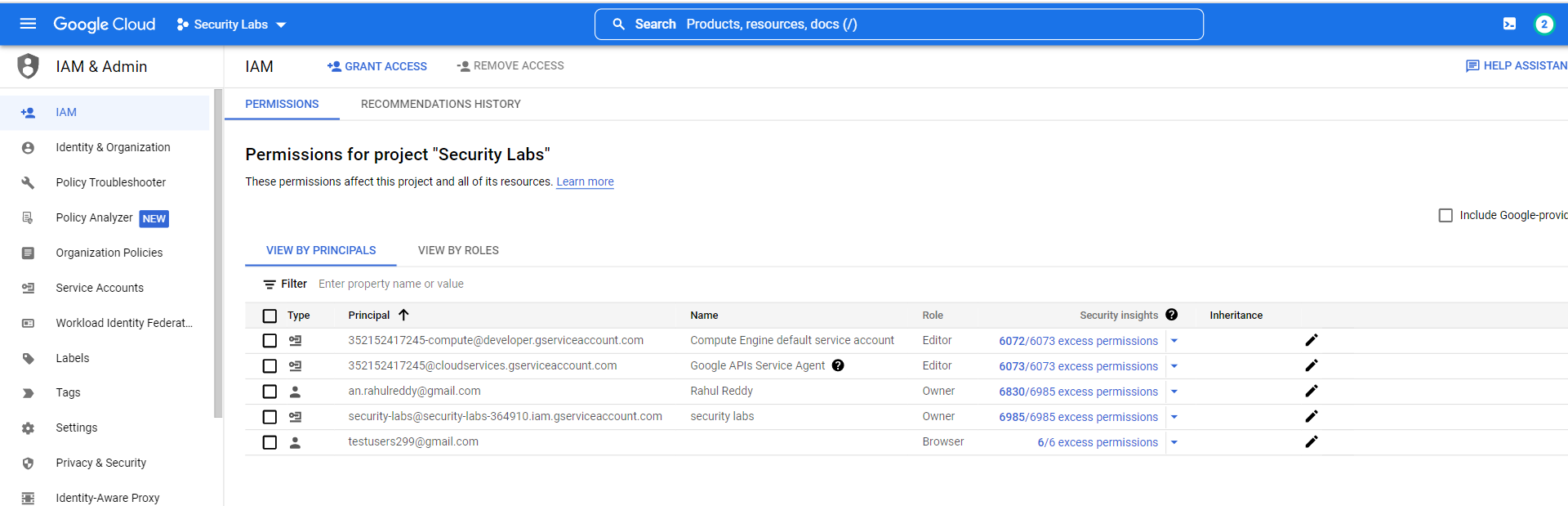
1. Your screen should look similar to this with project info changed to “*Security Labs”* project.



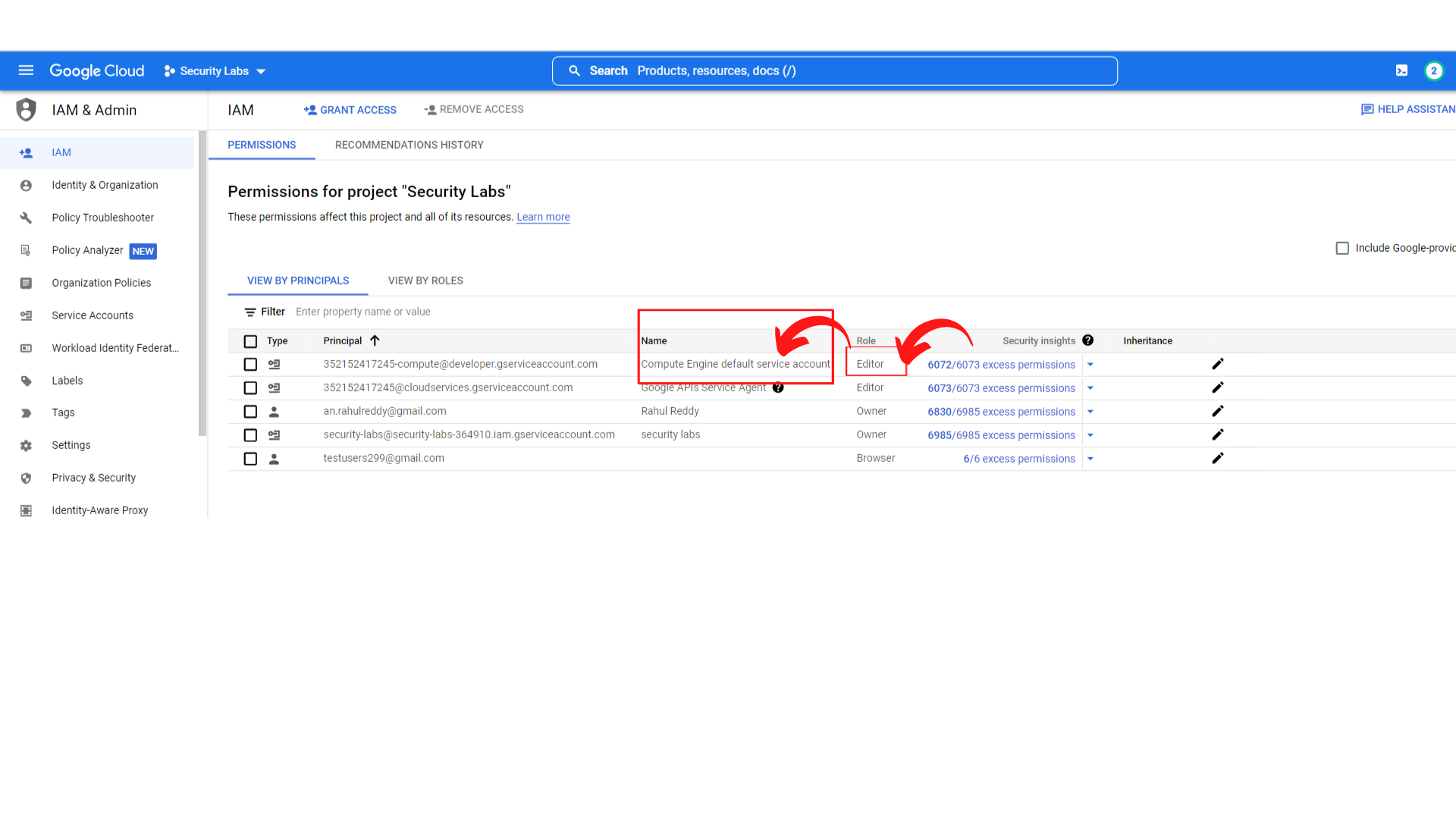
1. Click on *“Navigation menu”* on top left, then click on *“IAM & Admin ” → “IAM”*



1. Your screen should look similar to this.



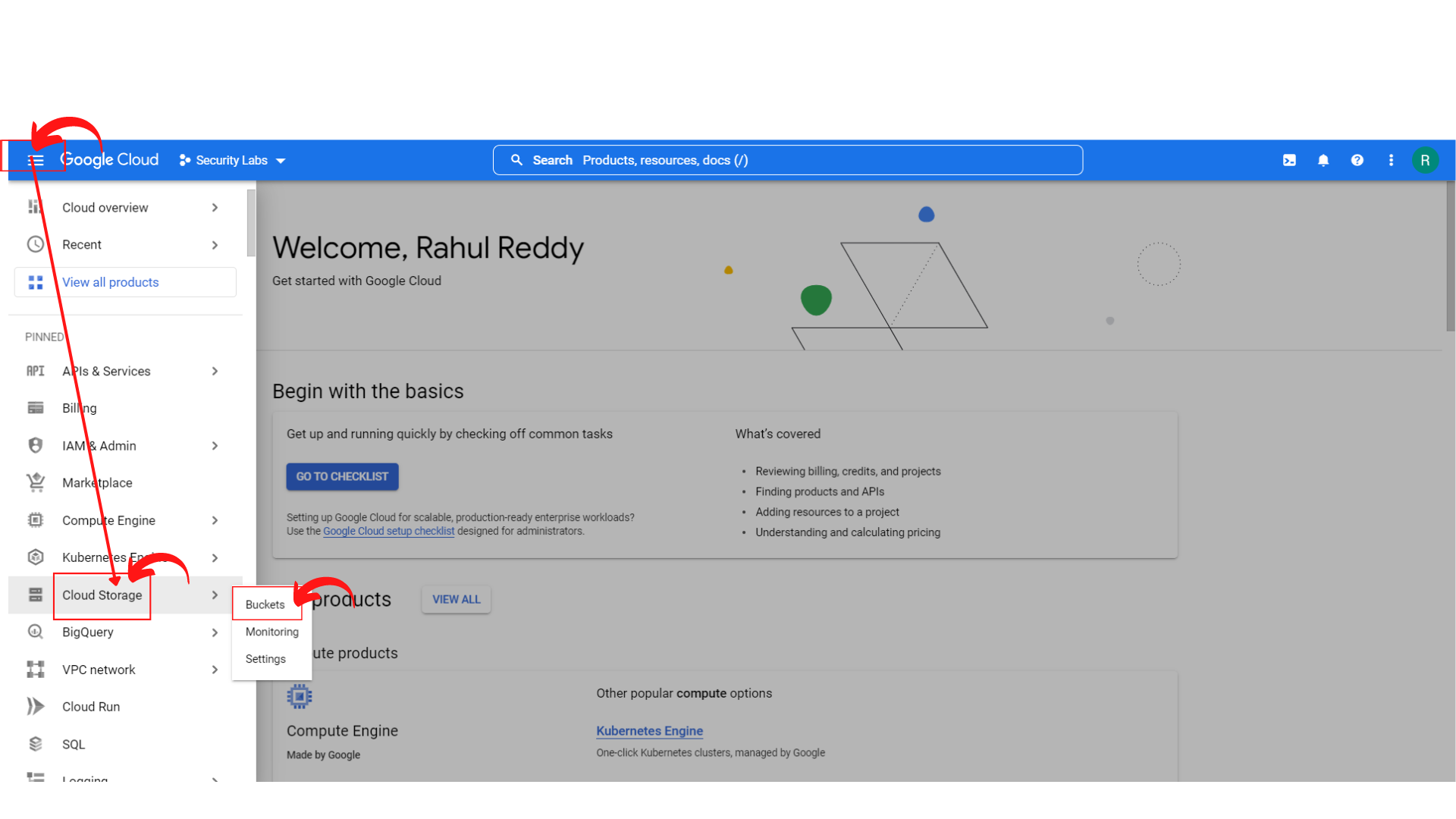
1. You need to verify that the ***Compute Engine default service account*** member has the ***Editor*** Role. You can see the screenshot below.



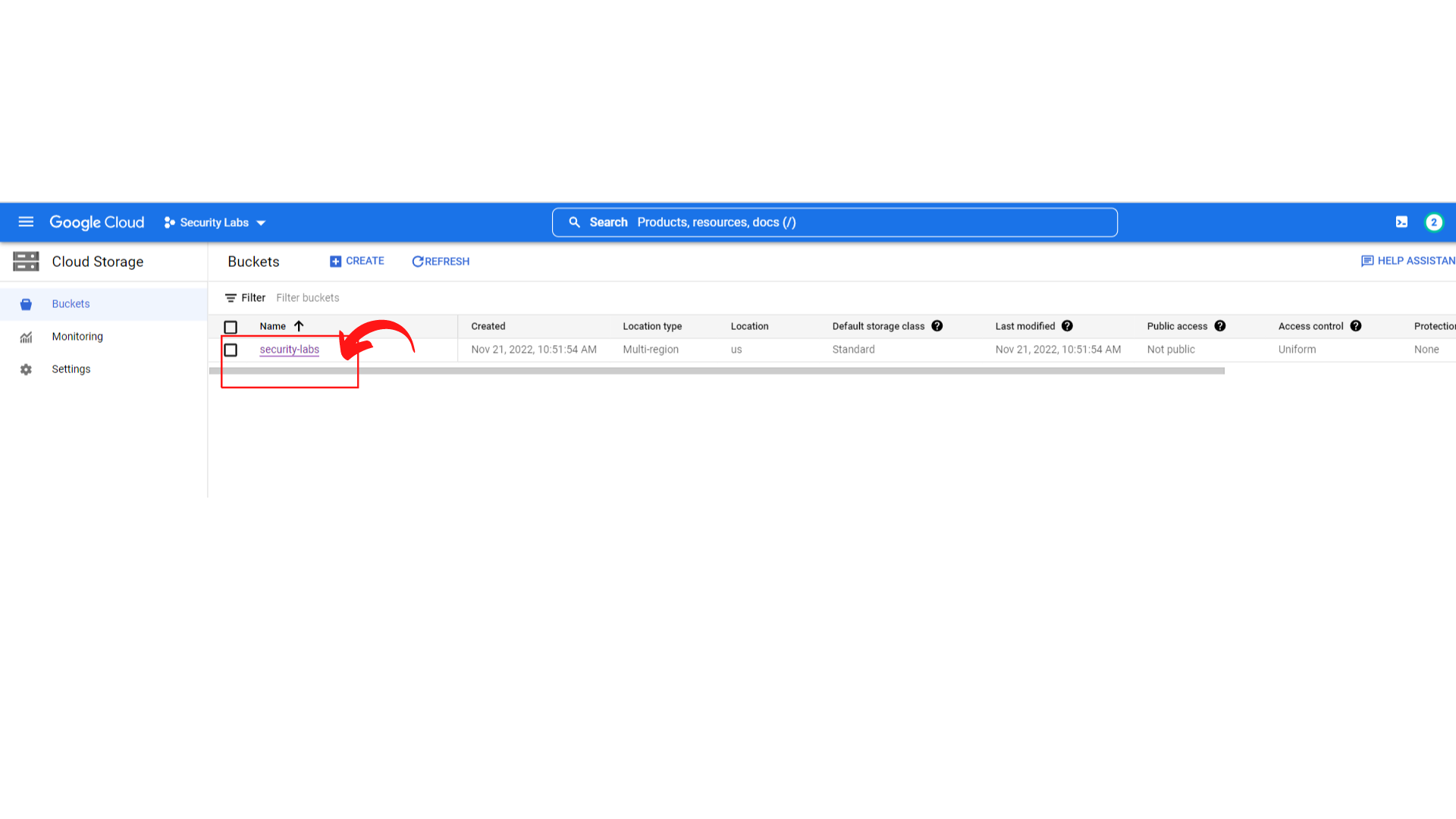
After Verifying that the Compute Engine default service account member has the Editor Role. Move to Step2.

**Step2:** Now you need to ***verify you have a storage bucket in your project***. If you do not have a storage bucket, please create a storage bucket.

1. Click on *“Navigation menu”* on top left, then click on *“Cloud Storage” → “Buckets”*



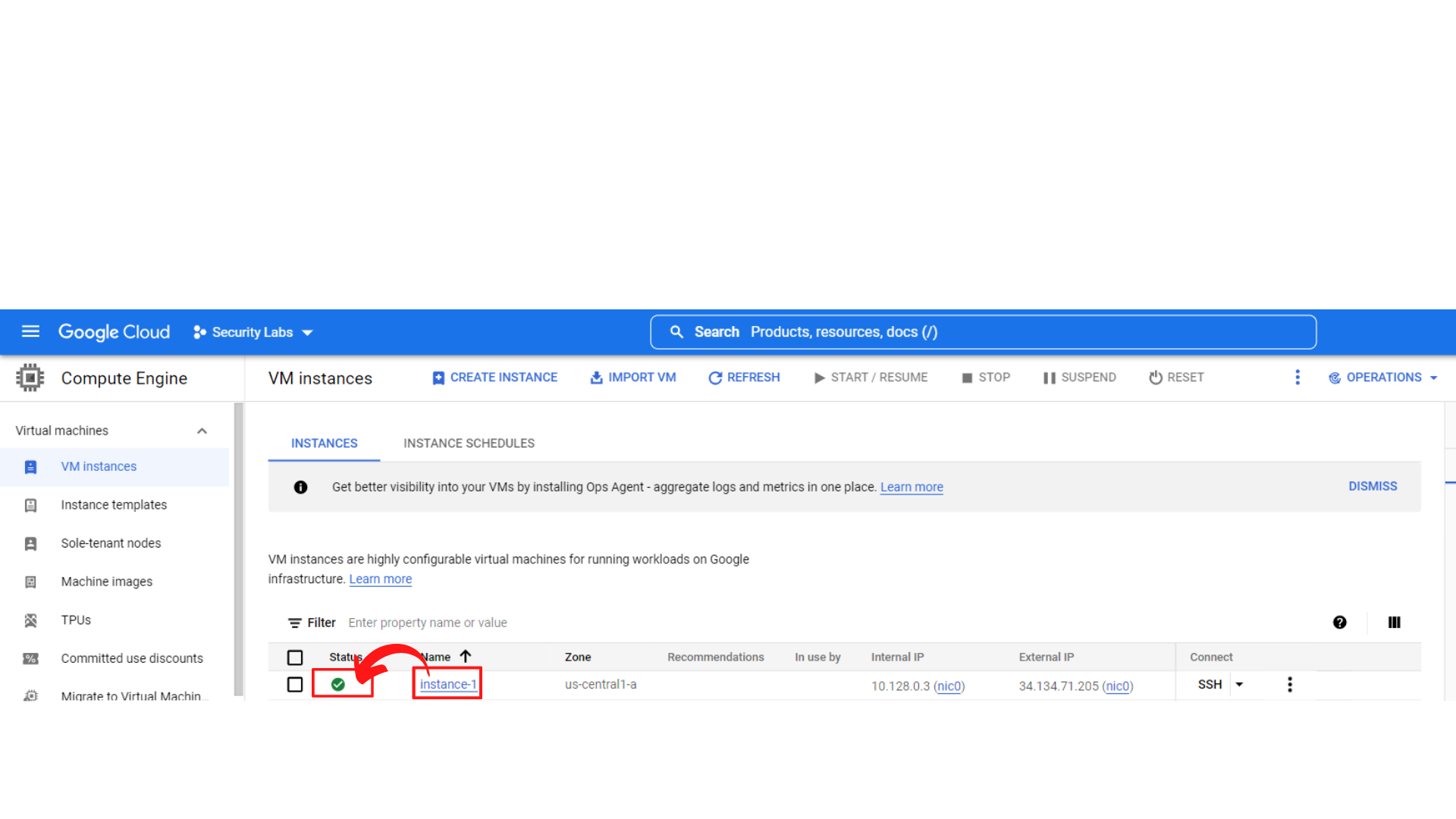
1. Your screen should look similar to this with a storage bucket. If you haven’t created a storage bucket, please create a new one.



After verifying that the storage bucket has been created, now you have to create a new instance with Read-only Storage Scope in Step3.

**Step3:** Now you need to ***Create a First Instance with Read-only Storage Scope.***

**There is a Document to create Instance-1 with Read-only Storage Scope. Please follow the instructions from the Document and create it.**

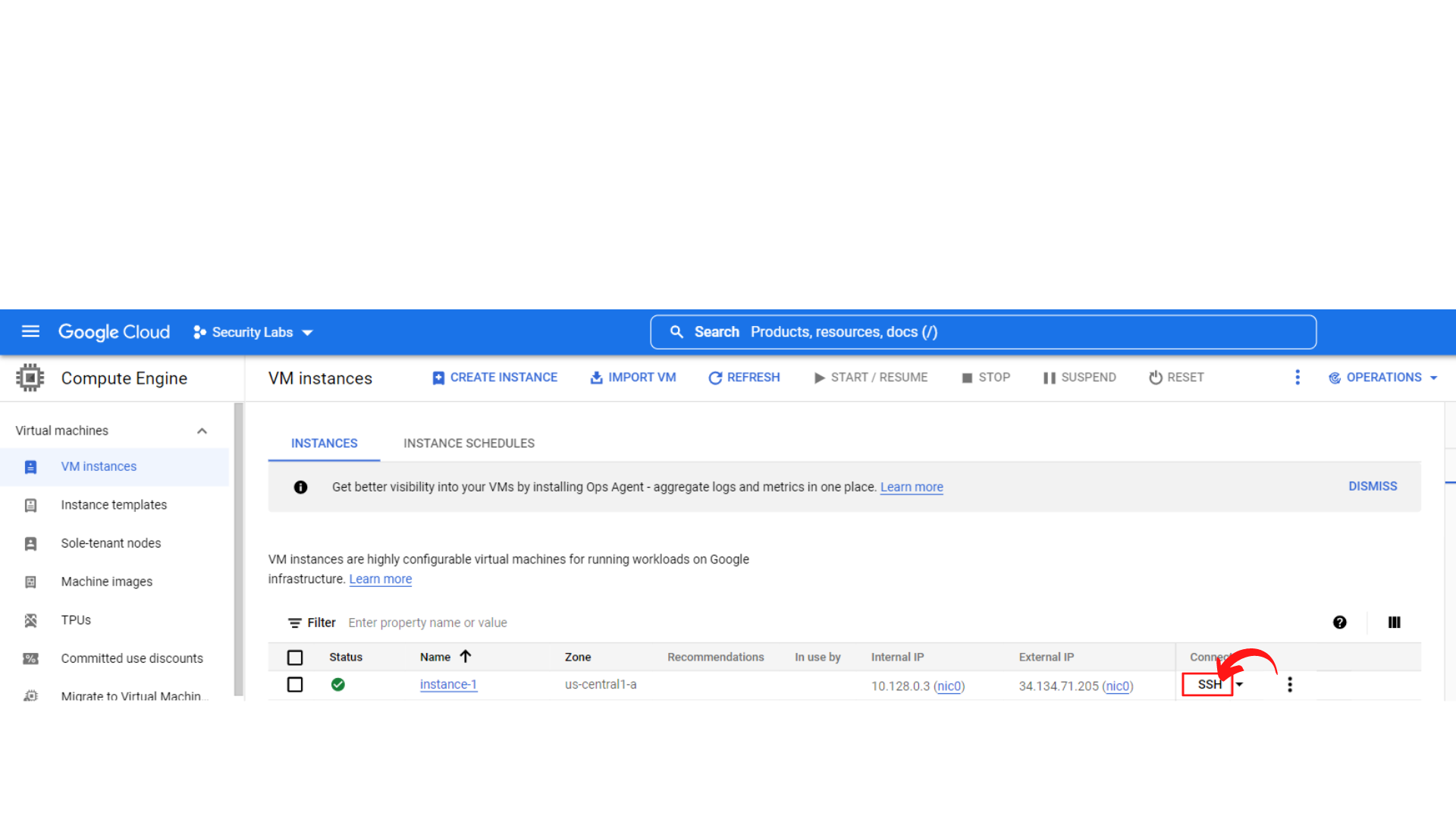
****

**Step4:** Now you need to Open the SSH and read and write the contents of the cloud Storage Bucket.

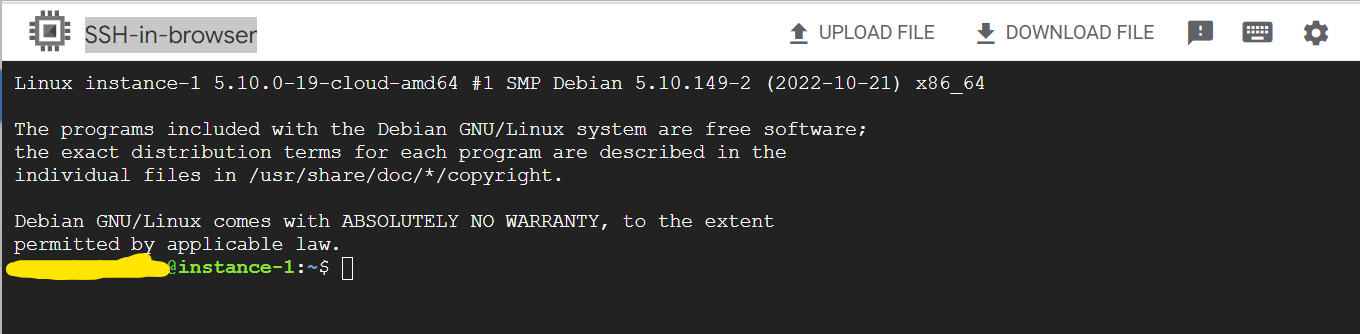
**Read** → We should access to read the contents.

**Write** → *We should not be able to write the contents since this instance has read-only access for storage scope*.

1. Your screen should look similar to this once the instance-1 has been created. ***“Click → SSH”***, this will open a new browser window with SSH-in-browser.

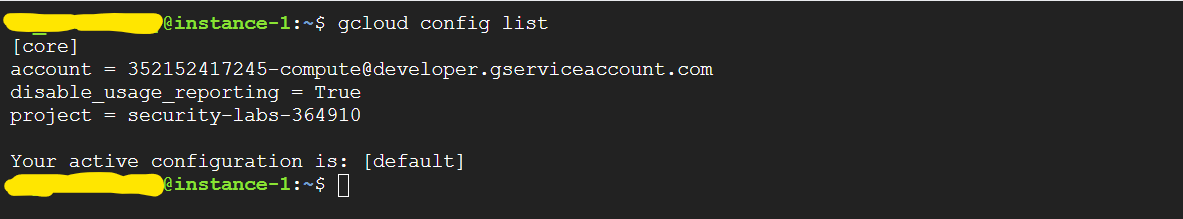


1. Your screen should look similar to this.



1. Now to view the Google Cloud SDK Configuration, Enter the following Command

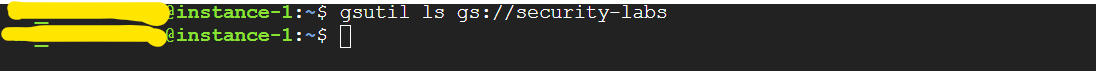
gcloud config list



1. Now Attempt to read contents from the Storage Bucket. Enter the following Command to read.

gsutil ls gs://BUCKET\_NAME

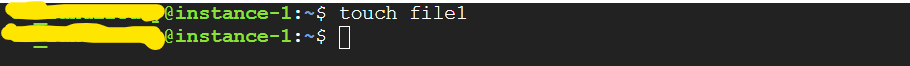
Note: Please replace BUCKET\_NAME with your Storage Bucket Name. Here my storage bucket name is security-labs.



1. Now Attempt to write a file to the same Storage Bucket. (This operation has to be failed since we haven’t given permission to write on this instance-1.)

Enter the following command to create a file with name file1

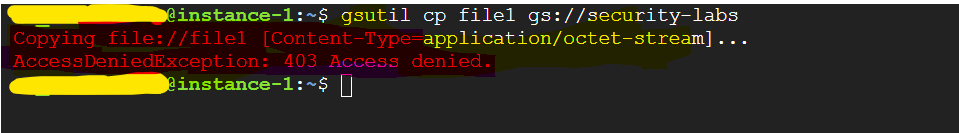
touch file1



1. Now trying to copy the file1 to the storage bucket. (This operation should fail)

Enter the following command

gsutil cp file1 gs://BUCKET\_NAME



You will see the 403 access denied since instance-1 doesn’t have permissions to read-only for storage bucket.